CLAIMS

What is claimed is:

1. A method comprising:

authenticating a user of a platform during a Basic Input/Output System (BIOS) boot process;

releasing a first keying material from a token communicatively coupled to the platform in response to authenticating the user;

combining the first keying material with a second keying material internally stored within the platform in order to produce a combination key; and

using the combination key to decrypt a second BIOS area to recover a second segment of BIOS code.

2. The method of claim 1 further comprising:

continuing the BIOS boot process.

3. The method of claim 1, wherein prior to authenticating the user, the method comprises:

loading a BIOS code including a first BIOS area and a second BIOS area, the first BIOS area being an encrypted first segment of the BIOS code and the second BIOS area being an encrypted second segment of the BIOS code.

4. The method of claim 3, wherein after loading of the BIOS code, the method further comprises:

decrypting the first BIOS area to recover the first segment of the BIOS code.

5. The method of claim 1 further comprising:

unbinding keying material associated with a non-volatile storage device to access contents stored within the non-volatile storage device.

6. The method of claim 1 wherein the combination key is a value formed by performing an exclusive OR operation on both the first keying material and the second keying material.

7. The method of claim 1, wherein authentication of the user is performed through biometrics.

8. The method of claim 1, wherein the second keying material is stored within internal memory of a trusted platform module.

9. The method of claim 1, wherein the second keying material is stored within a section of access-controlled system memory of the platform.

10. The method of claim 1, wherein prior to authenticating the user, the method comprises:

loading a BIOS code including a first BIOS area being a first segment of the BIOS code encrypted using a selected keying material; and

loading an integrity metric including a hash value of an identification information of the platform.

11. The method of claim 1, wherein the identification information includes a serial number of an integrated circuit device employed within the platform.

12. An integrated circuit device comprising:

a boot block memory unit; and

a trusted platform module communicatively coupled to the boot block memory unit, the trusted platform module to produce a combination key by combining a first incoming keying material with a second keying material internally stored within the integrated circuit and to decrypt a second BIOS area to recover a second segment of BIOS code.

13. The integrated circuit device of claim 12, wherein the boot block memory unit to load a BIOS code including a first BIOS area and a second BIOS area, the first BIOS area being an encrypted first segment of the BIOS code and the second BIOS area being an encrypted second segment of the BIOS code.

14. The integrated circuit device of claim 13, wherein the trusted platform module to decrypt the first BIOS area to recover a first segment of the BIOS code.

15. A platform comprising:

an input/output control hub (ICH);

a non-volatile memory unit coupled to the ICH, the non-volatile memory unit including a BIOS code including a first BIOS area and a second BIOS area, the first BIOS area being an encrypted first segment of the BIOS code and the second BIOS area being an encrypted second segment of the BIOS code; and

a trusted platform module coupled to the ICH, the trusted platform module to produce a combination key by combining a first incoming keying material with a second keying material internally stored within the platform and to decrypt the second BIOS area to recover the second segment of BIOS code.

16. The platform of claim 15, wherein the trusted platform module to further decrypt the first BIOS area to recover the first segment of the BIOS code in an non-encrypted format.

17. The platform of claim 15 further comprising a hard disk drive coupled to the ICH.

18. The platform of claim 17, wherein the trusted platform module to further unbind keying material associated with the hard disk drive to access contents stored within the hard disk drive.

19. A program loaded into readable memory for execution by a trusted platform module of a platform, the program comprising:

code to decrypt a first Basic Input/Output System (BIOS) area to recover a first segment of BIOS code;

code to produce a combination key by combining a first incoming keying material with a second keying material internally stored within the trusted platform module; and

code to decrypt a second BIOS area to recover a second segment of the BIOS code.

20. The program of claim 19, wherein the first BIOS area is the first segment of the BIOS code encrypted with a keying material and the second BIOS area is the second segment of the BIOS code encrypted with the combination key.

21. The program of claim 19 further comprising:

code to unbind keying material associated with a non-volatile storage device for accessing contents stored within the non-volatile storage device.